

## **REMARKS**

In the Office Action dated December 3, 2003, the Examining Attorney enumerates a number of objections and rejections as it relates to the this application. Each of these issues will be addressed in the same order as provided in the Office Action.

### **Information Disclosure Statement**

The applicant appreciates the Examiner reviewing the supplied Information Disclosure Statement and supporting documentation.

### **Specification**

The Examiner states that the Abstract exceeds 150 words. An amended Abstract is enclosed which has been amended to have fewer than 150 words. Specifically 145 words are now believed to be provided through the enclosed amendment to the Abstract.

### **Claim Rejections – 35 USC 112 Second Paragraph**

The Examiner has correctly observed a 35 USC 112 problem with Claim 29 as originally filed. Specifically claim 29 recited both a “second memory device” and a “third memory device.” The “third” memory device should have been a - - - second - - memory device for proper antecedent basis. The Examiner has correctly observed that these two elements are the same entity and this amendment is not believed to affect the substantive scope since the Examiner interpreted the claim as intended by the Applicant. The enclosed amendment removes reference to the “third” memory device.

## Claim Rejections – 35 USC 103 – Obviousness Rejections

The Office Action has proposed that claims 1 -16, 24-29, 31-33, 36-40 and 44 are obvious over Surf'N'Sign (an article by Herzberg and Naor, attached as Exhibit A) and Ganesan, U.S. Patent No. 5,535,276. The Applicant respectfully disagrees with this proposition as affected by the enclosed amendment.

Surf'N'Sign teaches a method for signing and authenticating electronic documents that differs at least in several areas from the claimed method of the applicant. First Surf'N'Sign teaches the use of a Netscape Navigator plug-in program which is installed on a local user's computer. Second Surf'N'Sign unequivocally requires signature computation to be performed locally at the client by code independent of the server:

...for client-based signature applications, the signature mechanism that has access to the signer's sensitive data (i.e., the private key) and that results in a commitment of the client, should be fully trusted....Hence it is logical to require that the software performing the signing operation must reside at the *client* and be a trusted piece of code *independent* of the server that contains the document to be signed. **For that reason, performing the signature at the server, by a Common Gateway Interference (CGI) for instance, is unacceptable."**

Another natural alternative is loading a Java applet from the server, while exploiting the trust mechanism of a signed applet supplied by the Java language. The problem with this solution is having access to the private key data of the signer - - it will require the private data to be sent repeatedly to the server. Moreover, the Java applet is not independent of the document being signed, since it is the same server that supplies both the signing code (applet) and the document."(emphasis added)(page 3-4)<sup>1</sup>

Thirdly, the Surf'N'Sign method does not teach "retrieval of private key portions associated with a plurality of users in a private key database on a local computer cluster".

---

<sup>1</sup> This application has been purchased by a new owner that lacks the Surf'N'Sign printout dated February 10, 2000. A new print out dated 5/13/04 having ten pages is enclosed as Exhibit A. The copy originally provided with the IDS apparently had twelve pages. The citations for this response are to Exhibit A which may be slightly different than to the originally provided copy of Surf'N'Sign. The new owner apologizes for any confusion.

Fourth, the Surf’N’Sign method explicitly “filters out HTML documents with active content since it does not intend to commit to the behavior of such components.”(p. 2)

Finally, as correctly observed by the Examiner, Surf’N’Sign does not disclose:

Retrieving at the local computer cluster a private key portion associated with the first user from the private key database generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key; and

Securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster.

The Ganesan reference describes a system and method for securing communications using split private key asymmetric cryptography. Specifically, each system user has an associated asymmetric crypro-key, such as an RSA crypro-key, with a public key portion and a corresponding private key portion. Each public key portion is known to the plurality of system users, and each private key portion has a **first private key portion**, which is preferably short in length, e.g. 8 to 12 characters, **known only to the associated user** and a corresponding second private key portion. (Ganesan, Col. 8, lines 11-18)

The first and second user communicate by having the first user generate a temporary private key portion and an associated temporary public key portion at the remote location of the first user. (Ganeson, Col. 8, lines 19-24). The temporary public key portion is encrypted with the first private key portion to form a first encrypted message. (Ganeson, Col. 8, lines 24-27). A third user, such as a local computer cluster, obtains the temporary public key portion by applying the second private key portion, typically retrieved from a secured database and the public key portion of the first user crypto-key to the first encrypted message. (Ganeson, Col. 8, lines 28-32). This entity can also issue a certificate.

The Ganesan method teaches the ability for the ability to provide a third party (the local computer cluster) to provide the function of authentication of one party to another through the

use of a secure database of private key portions. Signing of messages is also contemplated (Col. 9, line 55-67). Furthermore, Ganesan teaches the generation of a first private key portion at the remote computer (Col. 15, lines 45-50). Without the capability of generating the first private key portion at the remote computer, the process of Ganesan is not possible, as there is no way for the local computer cluster to authenticate the remote computer without the first private key portion being generated at the remote computer.

In the Background of the Invention of the specification as originally filed, the prior art public/private key method is described on page 1, line 20 – page 2, line 21. The only apparent difference between the method disclosed in the Background of the Invention and Ganesan appears to be the ability to recall a second private key portion from a database at a local computer cluster to use with a first private key portion provided from a remote computer.

Amendments to the claims, and/or discussions related to each claim provided below, will distinguish the applicants claimed methods from the prior art methods.

### **Claims 1, 25 and 36**

The Examiner proposes that claim 1 as originally filed is obvious over Surf'N'Sign in view of Ganesan. Specifically, the Examiner states: "Ganesan teaches that is advantageous for a trusted third party to maintain one portion of every user's RSA private key (Col. 3, lines 17-25). This forces the user to interact with a trusted third party, which provides practical advantages such as instant revocation."

The Office Action continues...: "it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Ganesan within the system of Surf because interacting with a trusted third party by allowing it to do the signing improves

the overall security of the system to all parties involved. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.”

The Office Action fails to establish a prima facie case of obviousness of claim 1. MPEP 2143 establishes the criteria for a prima case of obviousness. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant’s disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d1438 (Fed. Cir. 1991).

Surf’N’Sign requires that the software performing the signing operation must reside at the client (i.e., remote computer) and be a piece of code independent of the server that contains the document to be signed. **“For that reason, performing the signature at the sever....is unacceptable.”** (Surf’N’Sign, pages 3-4)(emphasis added).

Surf’N’Sign teaches that the claimed method of claim 1 is “unacceptable” since the signing occurs at the local computer cluster, such as a server. Nevertheless, through the use of the applicant’s disclosure, the Office Action attempts to transform Surf’N’Sign into a teaching which when combined with Ganesan would render the claimed method of claim 1 “obvious.” As explained by *In re Vaeck*, this fails to meet the three pronged test for establishing a prima facie case of obviousness of claim 1 as originally filed. Furthermore *In re Rinehart*, 541 F.2d 1048, 189 USPQ 143 (CCPA 1976) also discusses that there can be no reasonable expectation of

success when one of the references and the knowledge in the art teaches against the claimed method.

### **Claim 1**

Nevertheless, claim 1 has been amended to require that the signing request be generated in the absence of a pre-installed add-in software program on the remote computer and clarified so that the signature ready document is signed at the local computer cluster (instead of on the local computer cluster).

Surf'N'Sign teaches that the software performing the signing must reside at the client (the remote computer). Furthermore Surf'N'Sign teaches that "performing the signature at the server [local computer cluster]...is unacceptable."

Support for this amendment may be found in the specification as originally filed at page 8, line 17 – page 9, line 14. A pre-installed add-in software does not include programs such as Netscape Navigator or Microsoft Internet Explorer, but does include those programs dedicated software programs designed to remotely allow the user to access and sign documents at the local computer such as plug-in modules for use with the Navigator™ or Explorer™ modules.

Accordingly, as amended claim 1 is not rendered obvious by the combination of Surf'N'Sign and Ganesan. Allowance of independent claim 1, and its dependent claims 2-23 is respectfully requested on this basis.

### **Claim 25**

Claim 25 has been clarified to require that the complete private key is generated at the local computer cluster, if not provided as such from the private key database. Furthermore, and more importantly, the signing of the signature ready document has been amended to occur at instead of on the local computer cluster. Finally, claim 25 as amended requires the complete key

generated at the local computer cluster and independently of a private key provided by the user at the first remote computer.

Once again, Surf’N’Sign teaches that this would be “unacceptable.” Accordingly the proposed combination of Surf’N’Sign and Ganeson does not render amended claim 25, nor its dependent claims 26-34 obvious. Allowance of these claims is respectfully requested.

### **Claim 36**

Claim 36 has been clarified to require that the complete private key is generated at the local computer cluster if not provided as such from the private key database. Furthermore, and more importantly, the signing of the signature ready document has been amended to occur at instead of on the local computer cluster.

Once again, Surf’N’Sign teaches that this would be “unacceptable.” Accordingly the proposed combination of Surf’N’Sign and Ganeson does not render amended claim 36, nor its dependent claims 37-42 obvious.

As a separate basis for allowance, claim 36 has been amended to require that the “means for retrieving at the local computer cluster a private key portion associated with the first user from the private key database” occur independent of receiving both a public and a private key portion from the first user. Ganesan requires the provision of both a public key portion as well as a private key portion from the remote computer (i.e. client, user). The Ganesan method does not work without both keys. The combination of Ganesan and Surf’N’Sign does not render amended claim 36, nor its dependent claims 37 – 45 obvious. Allowance of these claims is respectfully requested.

## **Claim 2**

Claim 2 has been rejected with the statement: “Surf teaches the private key portion is a complete private key (pg. 7).” Claim 2 depends from claim amended claim 1 and is allowable for the reasons provided above for claim 1.

Additionally, when examining the antecedent basis of “the private key portion”, the Patent Office will observe that “the private key portion” is obtained from the private key database. This has been described as being unacceptable in the Surf’N’Sign system. (pp. 3-4) Accordingly, any combination with Surf’N’Sign cannot teach or suggest obtaining a complete private key from a private key database. Allowance of claim 2 is respectfully requested.

## **Claim 3**

The Office Action states:

Surf teaches receiving signing identification credentials for the first user (pgs. 6-7). Surf fails to teach constructing a complete private key using the private key portion and the received signing identification credentials. Ganesan teaches constructing a complete private key using the private key portion and received signing identification credentials (column 12, lines 45-65 and column 14, lines 10-40) The examiner supplies the same rationale for the motivation to incorporate the teachings of Ganesan within the system of Surf as recited in the rejection of claim 1. Surf teaches sending identification credentials to the server. Furthermore, it would have been obvious to one of ordinary skill in the art to generate the server side of the private key with identifying credentials because it associates the key with the intended user.

Claim 3 has been affected by the amendment to claim 1 and is allowable on that basis.

As a separate grounds for allowance, claim 3 has been amended to require that “signing credentials” are received at the local computer cluster from the first user at the remote computer after receiving the signing request. Ganesan only teaches a method for providing information to generate public and private keys in Col. 14, lines 10 – 40. Neither Ganesan nor Surf’N’Sign



teach receiving identification credentials after receiving a signing request. Accordingly, as affected by the enclosed amendment, claim 3 is separately allowable on this basis as well.

#### **Claim 4**

Claim 4 has been rejected on the basis that: “Surf teaches the received signing request was transmitted from the first remote computer to the local computer cluster over the internet (pg. 4). Claim 4 stands or falls with amended claim 1.

#### **Claim 5**

Claim 5 has been rejected on the basis that: “Surf teaches the received signing request was transmitted from the first remote computer to the local computer cluster over the world wide web using a hypertext transport protocol, and wherein the signing request was transmitted using a browser running on the remote computer (pg. 4).

Claim 5 depends from claim 1 and is allowable for the reasons provided above for claim 1. As a separate basis, the signing action is performed at the remote computer in Surf’N’Sign. Signing at the local computer cluster is described by Surf’N’Sign as unacceptable. Accordingly, it is not believed to be possible for Surf’N’Sign to transmit a signing request to the local computer cluster in accordance with that reference. Surf’N’Sign performs the signing at the remote computer. There is no need in Surf’N’Sign to send a request for the remote computer cluster to perform the signing for the user.

Accordingly, there is no support for establishing a prima facie case of obviousness as suggested by the Office Action. Allowance of claim 5 is respectfully requested.

### **Claims 6 and 33**

Claims 6 and 33 have been rejected on the basis that: “Surf teaches the retrieving at the local computer cluster the signature ready document is automatic (pgs 6-7). Claims 6 and 33 stand or fall respectively with claims 5 and 25.

### **Claims 7 and 32**

Claim 7 and 32 have been rejected on the basis that: “Surf teaches the retrieved signature document is standard generalized markup language document (pg. 4). Claims 7 stands or fall respectively with claim 6.

Claim 32 has been amended to require that the document be provided with the signing request, and activation of the signing request by the user sends the signing request from the remote computer to the local computer cluster. Support for this amendment may be found in page 14, lines 9-18 of the specification as originally filed. Surf’N’Sign has expressly provide that active content is filtered out of signed documents by Surf’N’Sign (p. 2). Accordingly no such link request could be transmitted by the Surf’N’Sign method. Accordingly, claim 32 is separately allowable on this basis as affected by the enclosed amendment.

### **Claims 8, 26 and 37**

Claims 8, 26 and 37 have been rejected on the basis that: “Surf teaches storing the signature ready document in a first document database (p. 6).” Claim 8 and 37 stand or fall respectively with claim 1 and 36. Furthermore, Surf teaches on page 6 the storage of signed documents in a database. The Applicant is unable to find a reference to a database in Surf for “signature ready documents.” This provides an additional basis for allowance of claims 8, 26, and 37.

Claim 26 requires a second remote memory device having stored thereon a signature ready document database, wherein the second memory device is remotely connected to the local computer cluster. This element has not been addressed by the Office Action. Accordingly, the third element of a prima facie case of obviousness has not been met as it relates to this claim. This element is not shown, described or taught by Surf'N'Sign, Ganesan, or the combination of the two. In addition to being allowable as depending from allowable claim 25 as discussed above, allowance of claim 26 on this basis is respectfully requested.

### **Claims 9 and 31**

Claims 9 and 31 were rejected on the basis that: "Surf teaches prior to signing: receiving form data from the first remote computer; and modifying the retrieved signature ready data based on the received form data (pgs. 2-4).

Unfortunately, there is no such reference in the Surf'N'Sign reference as proposed by the Office Action. Surf'N'Sign "adopts 'what you see is what you sign.'" (p. 2). There is no provision in Surf'N'Sign to modify documents and then to sign the modified document as claimed. It is only with impermissible hindsight and the use of the applicant's disclosure that this obviousness rejection can be articulated by the Office Action. Claims 9 and 31 are allowable and such action is respectfully requested.

Furthermore claim 31 has been clarified to ensure that "form data" does not include signing credentials, public key, or private key information. "Form data" is intended to relate to information provided to be placed on the signature ready document apart from signature information as provided by the specification as originally filed (page 13, line 21 – page 14, line 18). There is no support in either Ganesan or Surf'N'Sign for this element. Claim 31 is separately allowable on this basis as well the rationale provided above for claim 25.

Claim 9 depends from claim 8 and is allowable for the reasons articulated above for claim 8.

### **Claims 10 and 27**

Claims 10 and 27 have been rejected by the Office Action with the statement: “Surf teaches the first document database is located on the local cluster (pg. 6).” Page 6 of Surf’N’Sign appears to teach the existence of a document database of signed documents, not signature ready documents. Accordingly, there is no support in Surf’N’Sign for this rejection. Accordingly, claims 10 and 27 are separately allowable on this basis.

Claim 10 depends from claim 8 and is allowable as a result of the arguments provided above for claim 8, as well.

Claim 27 depends from claim 25 and is allowable for the rationale provided above for claim 25, as well.

### **Claim 11**

The rationale for the rejection of claim 11 states:

Surf fails to teach the first document database is located on a secure second remote computer. Ganesan teaches the first document database is located on a secure second remote computer (see figure 2, element 140). Separating the responsibilities of entities protects the users from having to put all of trust in one entity. Ganesan teaches a system whereby the duties of the secure environment are broken up among participating servers. Therefore, if the trust of one entity is found to be compromised then the whole system is not compromised. Only the information of entity needs to be recreated.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Ganesan within the system of Surf because divvying up the trust among servers reduces the level of trust one must have with a particular server. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

The Applicant agrees that Surf’N’Sign fails to teach the first document database is located on a secure second computer. Ganesan only teaches the use of a secure database to store portions of

keys. No mention is made in Ganesan of storing signature ready documents in a secure database. No mention is made in Surf’N’Sign of storing signature ready documents, only signed documents. It is only with hindsight and the use of the applicant’s disclosure that such a rejection can be formulated. This is an improper rejection. Claim 11 is separately allowable as the element is not taught or suggested in the cited prior art. Claim 11 also depends from claim 8 and is allowable on the basis provided above for claim 8.

#### **Claims 12, 28, and 38**

The rationale provided for the rejection of these claims states: “Surf teaches storing the signed document in a second document database (pg. 6).” Claims 12, 28 and 38 depend from claims 8, 25 and 37 and are allowable for the reasons provided above, respectively, for those claims.

#### **Claims 13 and 29**

Claims 13 and 29 were rejected by the Office Action through the rationale: “Surf teaches the second database is located on a secure second computer remote computer (pg. 6).” Claim 13 depends from claim 12 and claim 29 depends from claim 25. Claims 12 and 25 are allowable as discussed above.

#### **Claim 14**

Claim 14 was rejected by the Office Action through the rationale: “Surf teaches the second database is located on the local computer cluster (pg. 6).” Claim 14 depends from claim 12 and is allowable for the reasons provided above.

#### **Claims 15 and 39**

Claims 15 and 39 were rejected by the Office Action through the rationale: “Surf teaches associating at least one of the signature ready document and the signed document with a

document owner (pg. 6-7).” Claims 15 and 39 depend from claims 12 and claim 38, respectively and are allowable for the rationale provided above for those claims.

#### **Claims 16 and 40**

Claims 16 and 40 were rejected with the basis: “Surf teaches notifying at least one document owner and the first user that a signature ready document or a signed document has been signed (pg. 6). Claims 16 and 40 depend from claims 15 and 39, respectively and are allowable for the rationale provided above for those claims.

#### **Claim 24**

Claim 24 has been rejected. The rationale correctly observes that Surf “fails to teach to obtain a private encryption key associated with the identified user from a third remote computer.” Since Surf’N’Sign requires that the private key be generated on the remote computer and describes obtaining the private key from servers as “unacceptable”, there is no teaching or suggestion to obtain a key from another source. In fact, Surf’N’Sign teaches away from such a practice.

Ganesan does not teach signing a “retrieved document using the obtained private key” in the citation provided to (Column 12, lines 45-65 and column 14, lines 40). Ganesan teaches signing messages, not documents. Accordingly, it is only with hindsight that the rationale has been provided by the Office Action to improperly reject claim 24. Claim 24 is allowable as initially provided.

Nevertheless, claim 24 has been amended to require that the signing request sent from the remote computer to the local computer cluster be independent of both a public key and a private key portion. While the signature request could possibly contain either one of these two items, Ganesan requires transmission of both elements for the communication method taught therein.

The combination of Ganesan and Surf'N'Sign certainly does not suggest that claim, as amended, would be possible, or desirable. In fact, both references teach against such a practice.

Allowance of claim 24 is respectfully requested.

#### **Claim 44**

Claim 44 was rejected by the Office Action through the rationale: "Surf teaches the first user is a registered user (pg. 6)." Claim 44 depends from claim 36 and is allowable for the reasons provided above for claim 36.

#### **Obviousness Rejection of claims 17-21, 23, 30, 35, 35, 41, 42, 43 and 45**

Claims 17-21, 23, 30, 35, 35, 41, 42, 43 and 45 were rejected as being obvious over Surf'N'Sign and Ganesan as applied to claims 1 and 17 above, and in further view of Smithies et al, U.S. Patent No. 5,544,255. Smithies teaches a method and system for the capture, storage, transport and authentication of handwritten signatures (Title). Smithies does not teach associating digital signatures with handwritten signatures:

It is noted that the term "signature as used herein does not include what has become known in computer science fields as a "digital signature", i.e., an electronic code that is used to establish the identity of the person creating or sending an electronic document. A "digital signature" has the function of replacing a handwritten signature, with a secret alphanumeric "key" supplied to a given individual, which then has to be kept in secret. **In contrast**, the present invention is directed to electronically capturing a manipulating a person's handwritten signature. (Col. 3, lines 48-58) (emphasis added)

#### **Claims 17, 18, 41 and 42**

Claims 17, 18, 41 and 42 were rejected with the statement:

It would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Surf and Ganesan because the use of digital handwritten signatures is a way that a trusted server can viably authenticate a user. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

If the elements of claim 17 were examined as an independent claim (i.e., with **no** dependency to claim 1) only including those limitations which follow the “:” in claim 17, then Smithies does show each of these elements as a portion of the method of authenticating handwritten signatures.

However, apart from the Applicant’s disclosure and hindsight, there is no motivation to combine the teachings of a handwritten signature verification method with a method for electronically signing and authenticating documents. The Smithies reference as cited above distinguishes the two processes as being “**in contrast**” to one another.

Furthermore, there is still no motivation apart from the Applicant’s disclosure to combine Surf’N’Sign with Ganesan as explained above. Surf’N’Sign requires signing documents at the remote computer, while the claimed method requires signing at the local computer cluster. The Office Action fails to make a proper prima facie case of obviousness. Allowance of claim 17 is respectfully requested.

Claim 18 has been amended to require the recordation of at least one biometric measurement apart from a handwritten signature. As shown in the specification as originally filed at page 20, lines 21-23, the Applicant distinguished a person’s handwritten signature from “biometric data”. In searching the world wide web, it appears that at least some scholars propose that a handwritten signature provide biometric data. Nevertheless, as amended claim 18 now requires for additional biometric data to provided. Smithies is not believed to teach or suggest the capture and recordal of additional biometric data apart from handwritten signatures for any purpose. Accordingly claim 18 is separately allowable as amended on this additional basis.

If the elements of claim 41 were examined as an independent claim (i.e., with **no** dependency to claim 36) only including those limitations which follow the “:” in claim 36, then



Smithies does show each of these elements as a portion of the method of authenticating handwritten signatures.

However, apart from the Applicant's disclosure and hindsight, there is no motivation to combine the teachings of a handwritten signature verification method with a method for electronically signing and authenticating documents. The Smithies reference as cited above distinguishes the two processes as being "**in contrast**" to one another.

Furthermore, there is still no motivation apart from the Applicant's disclosure to combine Surf'N'Sign with Ganesan as explained above. Surf'N'Sign **requires** signing documents at the remote computer, while the claimed method **requires** signing at the local computer cluster. The Office Action fails to make a proper prima facie case of obviousness. Allowance of claim 36 is respectfully requested.

Claim 42 has been amended to require the recordation of at least one biometric measurement apart from a handwritten signature. As shown in the specification as originally filed at page 20, lines 21-23, the Applicant distinguished a person's handwritten signature from "biometric data". In searching the world wide web, it appears that at least some scholars propose that a handwritten signature provide biometric data. Nevertheless, as amended claim 42 now requires for additional biometric data to provided. Smithies is not believed to teach or suggest the capture and recordal of additional biometric data apart from handwritten signatures for any purpose. Accordingly claim 42 is separately allowable as amended on this additional basis.

#### **Claims 19 and 43**

Claims 19 and 43 have been rejected using a rather complicated, and improper argument. Specifically the Office Action states:

Smithies et al teach using the biometric measurements to determine whether individuals have previously registered (column 18, lines 1-23). Smithies

teaches that it is important to keep track of who has registered because only those that have registered can be granted access into the system. Therefore, it is obvious that the system must be able to distinguish new users from registered users. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Smithies et al within the combined system of Surf and Ganesan because Surf teaches registering users it would be advantageous to keep track of the users that have registered so that the system can distinguish new users from registered users. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

First, Smithies does not “teach using the biometric measurements to determine whether individuals have previously registered (column 18, lines 1-23).” Smithies teaches using “other information (surname, forename, middle names, user identification number)” to determine if a person has already registered. The first sentence of this paragraph begins: “When a client application 2 needs to create a template....” This means this process must occur before the template is created. Since the template has not been created, there is no way to compare the handwritten signature of the applicant with the handwritten signatures of others. Accordingly, Smithies does not teach using biometrics to determine whether individuals have previously registered. This Office Action has attempted to use the Applicant’s disclosure to assist in interpreting Smithies. This is improper.

Second, while Smithies may suggest it is important to keep track of who has registered, it certainly does not suggest using biometric data to perform that step as claimed. Claims 19 and 43 are separately allowable on this basis.

Furthermore claim 19 depends from claim 18, which depends from claim 17, which depends from claim 1. For the reasons provided above for those additional three claims, claim 19 is also allowable. Allowance of claim 19 is respectfully requested.

Claim 42 depends from claim 42, which depends from claim 41, which depends from claim 36. For the reasons provided above for those additional three claims, claim 43 is also allowable. Allowance of claim 43 is respectfully requested.

#### **Claim 20**

Claim 20 was rejected with the statement: “Surf teaches the first user is a registered user.” Claim 20 stands or falls with claim 17.

#### **Claims 21 and 45**

The Examiner correctly observes that: “Surf teaches appending a signature to a document but does not teach a digitized signature.” Surf teaches a method of remotely signing documents electronically. Smithies teaches a method of verifying handwritten signatures at a local computer cluster. Apart from applicant’s disclosure there is no teaching motivation to formulate a prima facie case of obviousness.

Through the methods of claim 21 and 45, a digital as well as a handwritten signature are associated with a signature ready document as a part of the signing step. There is no teaching or suggestion even through combining Smithies, Ganesan, and Surf’N’Sign to provide this claimed element. Accordingly, a prima facie case of obviousness has not been established. Allowance of claims 21 and 45 is respectfully requested.

Furthermore claims 21 and 45 depend from claims 17 and 45, respectively , and are believed to be allowable for the rationale articulated above for those claims.

#### **Claim 23**

Although claim 23 appears under the heading of rejections based on Surf’N’Sign, Ganesan and Smithies, the basis of the rejection appears to rely primarily on Surf’N’Sign and Ganesan.

Claim 23 requires the provision of handwritten signatures and recording identities of registered individuals through its dependency on claim 17 and the additional elements added with claim 23. Apart from the applicant's disclosure, if one skilled in the art were to examine Surf, Ganesan and Smithies, the claimed method of claim 23 would not be suggested. Surf does not mention an ability to handle handwritten signatures, neither does Ganesan. Smithies teaches the comparison of handwritten signatures with a stored version to create a checksum to authenticate whether or not the signature matches the stored version. It is only with hindsight and the applicant's disclosure that this rejection can be articulated. Allowance of claim 23 is respectfully requested.

Furthermore claim 23 depends from claim 17, and is believed to be allowable for the rationale provided above as it relates to claim 17.

### **Claim 30**

Claim 30 has been rejected under the rationale that: "it would have been obvious...to employ the teaching of Smithies within the combined system of Surf and Ganesan because it would allow the system a more secure method of authentication."

Both Surf'N'Sign and Ganesan provide for methods of authentication. To provide a "more secure method of authentication" as claimed is believed to be nothing more than the use of the applicant's disclosure and hindsight to formulate an improper obviousness rejection. There is no teaching or suggestion in the prior art to provide digitized handwritten signatures as claimed in claim 30 as a portion of an identity database related to the digital signature method claimed in claim 25. Claim 30 is separately allowable on this ground as well as the grounds articulated above for claim 25.

### **Claim 34**

Claim 34 has been rejected stating that it would have been obvious: “to employ the teaching of Smithies within the combined system of Surf and Ganesan because it would allow the system to prevent users who have not yet registered from using the system’s resources.” Smithies, Ganesan and Surf’N’Sign, separately or taken as a whole, do not teach or suggest a use of a registration computer with a digital signature system. While the Office Action attempts to use semantics to state: “One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success,” this is nothing more than using the Applicant’s disclosure as a roadmap to piece together unrelated references to attempt to formulate an obviousness rejection. This is improper.

Nevertheless, Surf’N’Sign and Ganeson cannot be combined as proposed by the Examiner as explained above for claim 25. Allowance of claim 34 is respectfully requested.

### **Claim 35**

The rejection states: “It would have been obvious ... to employ the teaching of Smithies et al within the combined system of Surf and Ganesan because digital handwritten signature are a way that a trusted server can viably authenticate a user.” Smithies teaches a method of authenticating handwritten signatures. Apart from the applicant’s disclosure there is no motivation, teaching or suggestion in the prior art for providing a second processor which records the identity of individuals, records digitized handwritten signatures, associates passwords with the digitized handwritten signatures, and stores appropriate information which can be utilized in conjunction with a digital signature system. It is only with hindsight that such a rejection is formulated.

Furthermore, claim 35 depends from claim 34 and is allowable for the rationale provided above for claim 34.

## **Claim 22**

Claim 22 has been rejected as being obvious over Surf, Ganesan, Smithies as applied to claims 1 and 17, and further in view of Shin, U.S. Patent No. 6,351,634. Shin relates to the a “Mobile Telephone and Method for Registering and Using Special Symbols as a password in same” (Title). Shin teaches a method of using special symbols as a password on a mobile telephone (remote computer). There is no teaching or suggestion in the cited portion Shin that the special symbols are displayed from a recognition graphics stored in an identity database on a local computer cluster at the remote computer. In fact the symbol data base in Shin is consistently referred to as a portion of the mobile telephone (remote computer) throughout column 1, line 60 – column 3, line 21.

Once again, it is only through the use of impermissible hindsight and the applicant’s disclosure as a roadmap that the rejection is formulated. Claim 22 is separately allowable on this basis as well as for the reasons provided above as they relate to claim 17, from which claim 22 depends.

## **Conclusion**

No additional claims have been made independent, no additional claims have been added. A petition for an extension of time for the third month and appropriate fee are enclosed. Allowance of pending claims 1-45 as affected by the enclosed amendment is respectfully requested.

Respectfully submitted,

Date: JUNE 2, 2004

By: 

Stephen J. Stark  
Attorney for Applicant  
MILLER & MARTIN LLP  
Suite 1000 Volunteer Building  
832 Georgia Avenue  
Chattanooga, Tennessee 37402  
(423) 756.6600

CERTIFICATE OF MAILING

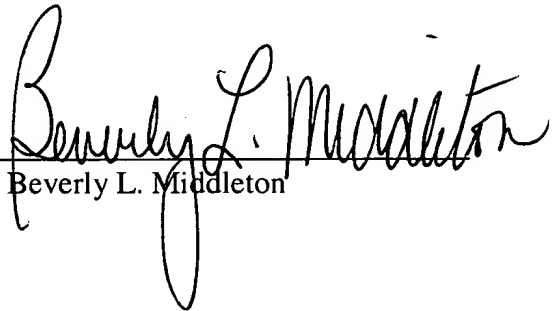
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Fee Amendment  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, Virginia 22313-1450

on this 2nd day of June, 2004.

By: \_\_\_\_\_

Beverly L. Middleton

A handwritten signature in cursive script, appearing to read "Beverly L. Middleton", written over a horizontal line.



**\*\*\* VERSION SHOWING CHANGED MADE \*\*\***

What is claimed is:

1. (Currently Amended) A method of signing and authenticating electronic documents comprising:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user said signing request generated in the absence of a pre-installed add-in software program configured to providing a signed message at the remote computer;

identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

retrieving at the local computer cluster a private key portion associated with the first user from the private key database;

generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key;

retrieving at the local computer cluster the signature ready document to be signed; and  
signing the signature ready document [on] at the local computer cluster using the generated complete private key to produce a signed document.

2. (Original) The method of claim 1 wherein the private key portion is a complete private key.

3. (Currently Amended) The method of claim 1 wherein generating a complete private key using the retrieved private key portion includes:

receiving signing identification credentials sent from the first user at the remote computer to the local computer cluster after receiving the signing request; and

constructing a complete private key using the private key portion and the received signing identification credentials.

4. (Original) The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the local computer cluster over the internet.

5. (Original) The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the local computer cluster over the world wide web using hypertext transport protocol, and wherein the signing request was transmitted using a browser running on the remote computer.

6. (Original) The method of claim 5 wherein the retrieving at the local computer cluster the signature ready document is automatic.

7. (Original) The method of claim 5 wherein the retrieved signature ready document is a standard generalized markup language document.

8. (Original) The method of claim 1 further comprising storing the signature ready document in a first document database.

9. (Original) The method of claim 8 further comprising prior to signing:

receiving form data from the first remote computer; and

modifying the retrieved signature ready document based on the received form date.

10. (Original) The method of claim 8 wherein the first document database is located on the local cluster.
11. (Original) The method of claim 8 wherein the first document database is located on a secure second remote computer.
12. (Original) The method of claim 8 further comprising storing the signed document in a second document database.
13. (Original) The method of claim 12 wherein the second database is located on a secure second computer remote computer.
14. (Original) The method of claim 12 wherein the second database is located on the local computer cluster.
15. (Original) The method of claim 12 further comprising associating at least one of the signature ready documents and the signed document with a document owner.
16. (Original) The method of claim 15 further comprising notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.
17. (Original) The method of claim 1 further comprising registering individuals as users, wherein registering includes:

verifying and recoding the identify of individuals registering;

digitizing and recording handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded identifies in an identify database, the identify database being accessible to the local computer cluster.

18. (Currently Amended) The method of claim 17 further comprising:

recording at least one biometric measurement[s] other than a handwritten signature of individuals registering;

associating the at least one biometric measurement[s] of individuals registering with the recorded identities of the individuals registering; and

storing the biometric measurements in the identity database.

19. (Original) The method of claim 18 further comprising detecting using the biometric measurements whether individuals previously registered.

20. (Original) The method of claim 17 wherein the first user is a registered owner.

21. (Currently Amended) The method of claim 20 wherein the signing comprises:

a) appending the first user's digitized handwritten signature to the signature ready document;

b) making a hash of the signature ready document; and

c) encrypting the hash of the signature ready document with the first user's private key.

22. (Original) The method of claim 17 further comprising:

associating and storing a secret set of recognition graphics with the passwords in the identity database;

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer;

requesting the first user to select graphics including in the secret set using a non-keyboard selecting device attached to the first remote computer;

receiving a message from the first remote computer identifying the selected graphics;

authorizing access to the local computer cluster if the selected graphics are included in the secret set.

23. (Original) The method of claim 17 further comprising:

generating the private key portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys;

associating the generated private key portions with the recorded identities of individuals registering; and

storing private key portions in a private key database.

24. (Currently Amended) A method of signing and authenticating electronic documents comprising:

running a browser on a first remote computer;

connecting to a local computer cluster via a computer network using the browser;

transmitting user identification information and document identification information to the local computer cluster; and

transmitting a signing request to the local computer cluster from the remote computer independent of both a private key portion and a public key portion, the signing request requesting the local computer cluster to retrieve the identified document from a second remote computer, to obtain a private encryption key associated with the identified user from a third remote computer, and to sign the retrieved document using the obtained private key on a fourth computer, wherein the first, second, third, and fourth remote computers can be the same computer or different computers.

25. (Currently Amended) A system for signing and authenticating documents comprising local computer cluster, the local computer cluster including:

a first memory device having a first program store thereon; and

a first processor coupled to the first memory, wherein the first processor can read the first program stored in the first memory and can perform the steps of:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

retrieving at the local computer cluster a private key portion associated with the first user from the private key database.

generating at the local computer cluster independent of a private key provided from the first remote computer a complete key using the retrieved private key portion of the retrieved private key portion is not a complete private key;

retrieving at the local computer cluster the signature ready document to be signed; and

signing the signature ready document [on] at the local computer cluster using the generated complete private key to produce a signed document.

26. (Original) The system of claim 25 further comprising a second remote memory device having stored thereon a signature ready document database, wherein the second memory device is remotely connected to the local computer cluster.

27. (Original) The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon a signature ready document database, wherein the second memory device is coupled to the processor.

28. (Original) The system of claim 25 further comprising a second memory device having stored thereon a signed document database, wherein the second memory device is remotely connected to the local computer cluster.

29. (Currently Amended) The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon a signed document database, wherein the [third] second memory device is coupled to the processor.

30. (Original) The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon an identity database, the identity database including user digitized handwritten signatures, recorded user identities associated with the signatures, and passwords associated with the user identifies.

31. (Currently Amended) The system of claim 25 wherein the processor can perform the additional steps of:

receiving form data independent of at least one of signing identification credentials, and public and private key information from the first remote computer; and

modifying the retrieved signature ready document based on the received form data.

32. (Currently Amended) The system of claim 25 wherein the received signature ready document [is a standard generalized markup language document] further comprises the signing request, and activation of the signing request at the remote computer transmits the signing request to the local computer cluster.

33. (Original) The system of claim 25 wherein the retrieving at the local computer cluster the signature ready document is automatic.

34. (Original) The system of claim 25 further comprising a registration computer connected to the local computer cluster.



35. (Original) The system of claim 34 wherein the registration computer comprises a second memory device having a second program stored thereon; and

a second processor coupled to the second memory, wherein the second processor can read the second program stored in the second memory and can perform the steps of:

recording the identify of individuals registering;

and recording digitized handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identify database being accessible to the local computer cluster.

36. (Currently Amended) A system for signing and authenticating documents comprising:

a means for securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

a means for receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

a means for identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

a means for retrieving at the local computer cluster a private key portion associated with the first user from the private key database independent of receiving both a public and a private key portion from the first user;

a means for generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key at the local computer cluster;

a means for retrieving at the local computer cluster the signature ready document to be signed; and

a means for signing the signature ready document [on] at the local computer cluster using the generated complete private key to produce a signed document.

37. (Original) The system of claim 36 further comprising a means for storing the signature ready document in a first document database.

38. (Original) The system of claim 37 further comprising a means for storing the signed document in a second document database.

39. (Original) The system of claim 38 further comprising a means for associating at least one of the signature ready document and the signed document with a document owner.

40. (Original) The system of claim 39 further comprising a means for notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.

41. (Original) The system of claim 36 further comprising a means for registering individuals as users, wherein the means for registering includes:

a means for verifying and recording the identity of individuals registering;

a means for digitizing and recording handwritten signature of individuals registering;

a means for associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

a means for storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster.

42. (Currently Amended) The system of claim 41 further comprising:

a means for recording biometric measurements other than the handwritten signature of individuals registering;

a means for associating the biometric measurements of individuals registering with the recorded identities of the individuals registering; and

a means for storing the biometric measurements in the identity database.

43. (Original) The system of claim 42 further comprising a means of detecting using the biometric measurements whether individuals have previously registered.

44. (Original) The system of claim 36 wherein the first user is a registered user.

45. (Original) The system of claim 44 wherein the means of signing comprises:

a) a means of appending the first user's digitized signature to the signature ready document;

b) a means of making a hash of the signature ready document; and

c) a means of encrypting the hash of the signature ready document with the first user's complete private key.